

REMARKS

The Examiner is thanked for the careful review of this application. Claims 1-26, 28 and 29 remain in this application. Claims 1, 15, and 26 have been amended.

Independent claims 1, 15, and 26 have been amended to require, *inter alia*, receiving first and second timing signals from a remote source using a receiver. In particular, both the first and second timing signals are generated from the same remote source and received using the same receiver. In addition, independent claims 1, 15, and 26 have been amended to require computing a delay number that is a measure of a variation between arrival times of the first and second timing signals at the receiver.

Claims 1-6, 15-22, 26, 28, and 29 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,659,617 to Fischer (hereinafter "the Fischer patent"). It is respectfully submitted that independent claims 1, 15, and 26, as amended, are allowable over the art of record.

In particular, the Fischer patent fails to teach each and every feature of independent claims 1, 15, and 26, as amended. Independent claim 1, as amended, provides a method for protecting electronic files that includes, *inter alia*, 1) receiving first and second timing signals from the same remote source using a receiver, 2) computing a delay number that is a measure of a variation between arrival times of the first and second timing signals at the receiver, and 3) creating an encryption key that is based on environment information of a computer, where the environment information includes data concerning the operating environment of the computer and the delay number.

Variations in the ionosphere and atmosphere due to weather, barometric pressure, solar activity, and other variable and unpredictable parameters generally cause the purity of the timing signals to fluctuate, causing unpredictable delays in the timing signals. Embodiments of the present invention utilize these variances in timing signals as a source for an unpredictable random number, which is referred to as the "delay number." The delay number is utilized as an unpredictable random number for use in protecting electronic files. Advantageously, the delay number depends on the moment to moment value of the various

parameters along the path from the satellite to the receiver. Therefore, the delay is specific to each satellite and receiver at a specific time and a specific location, and is extremely difficult, if not impossible, to calculate remotely, thus preventing hacking, breaking, deciphering, or otherwise “spoofing” the system.

The unpredictable nature of the delay number is utilized in claim 1, which recites: “receiving first and second timing signals from a remote source using a receiver.” Hence, claim 1 requires receiving two timing signals from the same remote source. Claim 1 also recites: “computing a delay number, the delay number being a measure of a variation between arrival times of the first and second timing signals at the receiver.” Hence, claim 1 defines the delay number as the variation between the arrival times of the first and second timing signals at the receiver. Again, it should be borne in mind that both timing signals are received from the same remote source.

The Fischer patent does not disclose “receiving first and second timing signals from a remote source using a receiver,” as required by amended independent claim 1. Quite to the contrary, the position determination unit (PDU) of the Fischer patent utilizes a plurality of signals from different sources to triangulate the position of the PDU. Nowhere in the Fischer patent is there disclosed receiving two timing signals from a single remote source.

Moreover, the Fischer patent does not disclose “computing a delay number, the delay number being a measure of a variation between arrival times of the first and second timing signals at the receiver,” as required by amended independent claim 1. Although the Fischer patent may utilize timing signals from remote sources to compute location, these are timing signals from different satellites. Nowhere in the Fischer patent is there disclosed measuring a variation between arrival times of two timing signals received from a single source. This is because the PDU of the Fischer patent cannot compute its location only utilizing timing signals from a single satellite. The PDU requires signals from at least three different satellites to triangulate its position.

Embodiments of the present invention utilize the delay number to protect electronic files, as illustrated in claim 1, which further recites: “obtaining environment information regarding a computer, the environment information including the delay number and data concerning an operating environment of the computer” and “creating an encryption key based

on the environment information.” Hence, the present invention protects electronic files by obtaining the operating environment of the computer and utilizing it, in conjunction with the delay number, to create an encryption key, which is then used to encrypt an electronic file.

To decrypt the file at a later date, the same encryption key needs to be regenerated. However, if any factor of the environment profile changes, the regenerated key will be different from the key used to encrypt the file because the environment profile on which the regenerated key is based will be different. As a result, the regenerated key will be unable to decrypt the file. For example, if the encrypted file is moved to another computer, the environment information of the other computer will not match the environment information used to generate the encryption key which was used to encrypt the file. As a result, when the other computer generates the new encryption key, the generated encryption key will not be able to decrypt the file, hence protecting the file from unauthorized access.

Unlike the present invention, the Fischer patent does not disclose using computer environment information to create an encryption key. The Fischer patent uses a pre-designed encryption key to encrypt the location information provided by the PDU unit, but does not disclose creating an encryption key based on the environment information, as required by independent claim 1. Indeed, the Fischer patent does not disclose creating an encryption key at all, much less creating an encryption key based on characteristics of the computer’s operating environment.

Accordingly, independent claim 1 is submitted to be patentable under 35 U.S.C. § 102 over the Fischer patent. Claims 2-14, each of which ultimately depends from independent claim 1, are likewise submitted to be patentable under 35 U.S.C. § 102 over the Fischer patent for at least the same reasons set forth above regarding claim 1. Furthermore, independent claims 15 and 26, and dependent claims 16-25, and 28-29, respectively, are submitted to be patentable over the art of record for at least the same reasons as set forth above with respect to claim 1.

In view of the foregoing, the Applicant respectfully submits that all pending claims in the present application are in condition for allowance, and a notice of allowance is

Appl. No. 10/003,572
Amdt. dated October 12, 2005
Reply to Office action dated July 12, 2005

respectfully requested. In the event a telephone conversation would expedite prosecution of this application, the Examiner may reach the undersigned at (909) 758-5145.

Respectfully submitted,
PATENT VENTURE GROUP

A handwritten signature in black ink, appearing to be 'Joe A. Brock II', written over a horizontal line.

Joe A. Brock II, Esq.
Reg. No. 46,021

PATENT VENTURE GROUP
10788 Civic Center Drive, Suite 215
Rancho Cucamonga, California 91730
(909) 758-5145
Customer No. 52785